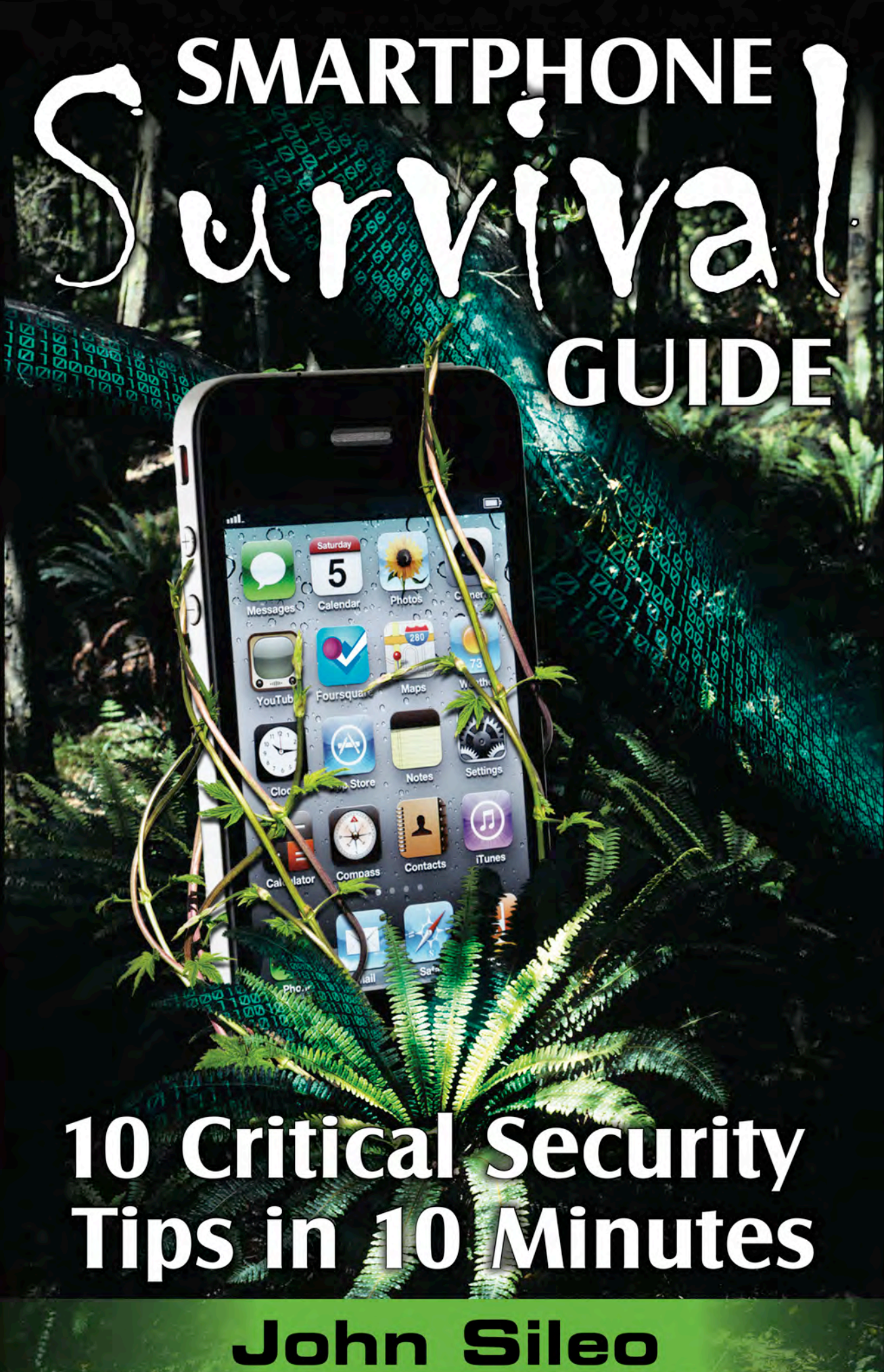


SMARTPHONE Survival GUIDE

A central image of a smartphone with its screen on, displaying various app icons like Messages, Calendar, Photos, YouTube, Foursquare, Maps, Weather, Clock, App Store, Notes, Settings, Calculator, Compass, Contacts, and iTunes. The phone is surrounded by lush green ferns and vines. The background is a dark, dense forest with a green binary code overlay.

**10 Critical Security
Tips in 10 Minutes**

John Sileo

Copyright © 2011 by John Sileo. All rights reserved Published by The Sileo Group, Inc., Denver, Colorado

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher.

Requests to the Publisher for permission should be addressed to the Permissions Department, The Sileo Group, 381 S. Broadway, Denver, CO 80209, (303) 777-3222, fax (866) 422-4922.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

To obtain a copy of this workbook in other formats, please visit www.ThinkLikeASpy.com. For bulk purchases, please contact The Sileo Group directly on (800) 258-8076.

Smartphone Survival Guide

10 Critical Security Tips in 10 Minutes

Table of Contents

Smartphone Survival Guide <i>10 Critical Security Tips in 10 Minutes</i>	ii
Immediate Action-Items	1
Your Smartphone is as Powerful and Dangerous as a Computer	3
1. Lock It Up and Don't Lose It!	3
2. Turn on Password Protection.	4
3. Enable Remote Tracking and Wiping Capabilities.	5
4. Install Security Software	6
5. Load Data with Discretion.	7
6. Minimize Unnecessary Application (App) Spying	8
7. Turn on Data Encryption	11
8. Hold off on Mobile Banking and Investing	11
9. Customize Your Geo-Tag and GPS Settings	12
10. Use Tethering and Mobile Account Alerts to Your Advantage.....	14
A Crash Course in Expanding Mobile Security into the Workplace.....	17
About the Author	Error! Bookmark not defined.

Important Note

For all of the Smartphones and Operating Systems (also referred to as OS) discussed in this workbook, be sure that you consult your operator's manual or online instructions for your particular handset and service provider, as there are numerous models and constant updates to settings and options. This is particularly true of the BlackBerry and Android phones, which work on many brands of handsets and are offered by a range of cell phone carriers. Here are a few websites to get you started:

Android

See Mobile Phone Manufacturer's Website

Apple

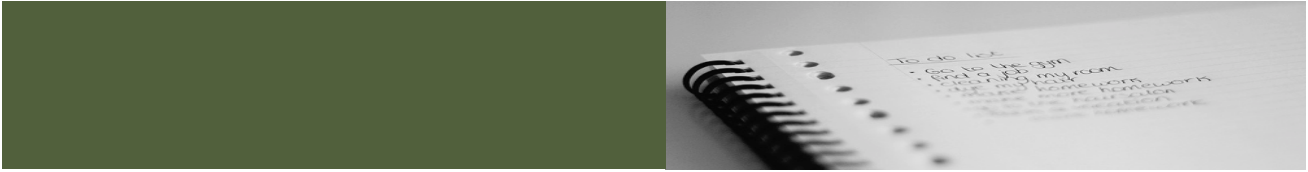
<http://support.apple.com/manuals/>

BlackBerry

http://docs.blackberry.com/en/smartphone_users/

Windows

<http://www.microsoft.com/windowsphone/en-us/howto/wp7/default.aspx>



By the time you have completed the following checklist, your Smartphone will be considerably more protected than the average phone, greatly reducing your risk of data theft. The Survival Guide shouldn't take more than 10-15 minutes to read through. As you are reading, circle the items below that you need to correct. Implementing each one may take a few additional minutes, but will be well worth it.

Immediate Action-Items

- ☐ Lock it up & don't lose it! (Step 1)
- ☐ Turn on password protection. (Step 2)
- ☐ Enable remote tracking & wiping capabilities. (Step 3)
- ☐ Install security software. (Step 4)
- ☐ Load data with discretion. (Step 5)
- ☐ Minimize unnecessary application spying. (Step 6)
- ☐ Turn on data encryption. (Step 7)
- ☐ Hold off on mobile banking & investing. (Step 8)
- ☐ Customize your geo-tag & GPS settings. (Step 9)
- ☐ Use tethering & mobile alerts to your advantage. (Step 10)

Your Smartphone is as Powerful and Dangerous as a Computer

As Smartphones (iPhone, BlackBerry, Droid, Windows Phone) have blurred the line between traditional mobile phones and fully equipped computers, data theft has gone increasingly mobile. In addition to carrying contact information on our phones, we now carry client files, banking logins, account information, sensitive emails, medical data and other private information, both personal and professional. Combining this computing powerhouse with mobility and travel makes it especially vulnerable to theft.

Just as we equip our computers with the latest in security technology and train our users to avoid fraud, so must we now protect our Smartphones in order to keep identity thieves, corporate spies and unwanted users out of our data. The following 10 Smartphone Security Tips will get you started.

1. Lock It Up and Don't Lose It!

Mobile phones are small and extremely easy to steal. In our push to be technologically savvy, we often forget that the first form of protecting Smartphones (or laptops, for that matter) is physical nature. Keeping your phone physically on you or locked up when not in use is the most basic form of protection. Don't set your phone down in a restaurant or bar even for a second (as someone at Apple found out when a pre-release prototype of the iPhone 4 was stolen). Many phones are stolen from café tables, coat pockets, shopping carts, airport security bins, taxis and cars while they are momentarily unattended or somehow left behind.



In addition, be careful to whom you loan your cellphone. I wish it weren't true, but a lot of the spying software is loaded in the few minutes that you let someone else have control of your phone. This unfortunately includes competitors and suspicious spouses who want to install Tapping software on the handset. For example, it takes about 30 seconds to load PhoneSnoop on a BlackBerry, allowing an outsider to turn on the microphone at any time completely undetected and listen to nearby conversations. Granted, the spy needs physical access to the phone, must know your password and probably can't physically hide the App. That in mind, I recently worked with a corporation whose competitor had installed this piece of spying software on the mobile phones of their top sales people while at an industry conference using a relatively simple Social Engineering scheme (that I won't share here).

If you loan out your phone, never share the passcode and make sure you are always with the person using it. The latest scam is for someone in a café or the airport to ask you to use the phone to make a quick local call. You think they are tapping away a number when they are actually installing a malicious App. The second most common way is for someone to send a

malicious link through an email address you recognize (the thief has taken over their email account), effectively getting you to do their dirty work for them.

Extra Tip: In case you do lose your Smartphone (statistically, the #1 way that Smartphones fall into the wrong hands), make sure that you have a recent backup or sync of the contents of your phone so that you don't lose that as well. Also, take a look at Step 3 to shut down the data before it is abused.

As you make it increasingly difficult to steal data off of your Smartphone, thieves will tend to move on to easier targets (unless there is something highly valuable on your phone and they know it). Managing to never lose or misplace your phone, of course, is nearly impossible, which is why there are 9 additional ways to protect your Smartphone.

2. Turn on Password Protection.

Most Smartphones have password protection features that can be turned on to help keep unwanted users out (or at least slow them down a bit). After a few moments of inactivity, the phone will auto-lock itself and require a password to get back in. This simple step goes a long way toward protecting the data on your phone and preventing a criminal from making calls on your dollar or thousands on the sensitive data you store there. If nothing else, passwords slow down the thief long enough to give you time to remotely “wipe” your memory (see Step 3). Make sure that your password is something easy to type and hard to forget. Don't make it simple (7777 or 1234), as thieves already know the most common combinations. But don't make it so long that it's difficult to enter on the fly. Stay away from birthdates, addresses, phone extensions and other easy to guess codes.

Here's how to set the time-out/password settings on various Smartphone operating systems (please note that these and other settings change frequently – look for updates on the individual operating system and handset websites):

- ☑ **Apple iOS (iPhone/iPad/iPod Touch):** Open the *Settings* app, select *General* and then *Passcode Lock*. Set your passcode here. Directly above the *Passcode Lock* is the *Auto-Lock* option (on newer versions of the OS), which turns the time-out on and off and let's you control the length of inactivity. For more details, visit: <http://support.apple.com/kb/HT4113>.
- ☑ **BlackBerry:** From the home screen, click *Options*, *Security Options*, *General Settings*. Once there, you can enable the feature, set or change the password, and set the security time-out options.
- ☑ **Android:** The later versions of Android support PINs and passwords. From the home screen, press *Menu*, *Settings*, *Security* (some androids are *Location & Security*), and under *Screen Unlock* you'll find several options for setting passwords. To set the screen time-out, however, you must return to the *Settings* menu and click *Display*. (Note: If you choose to go with the pattern unlock passcode, create a complex pattern



that crosses over itself so that thieves can't deduce your pattern from the smudge marks on your screen).

- ☑ **Windows Phone 7:** Open *Settings*, and then select *Lock* and *Wallpaper*. From there, you can set or change the password, and enable screen time-outs. You can also use a PIN to lock your SIM card and prevent people from making unauthorized phone calls. For more details visit <http://www.microsoft.com/windowsphone/en-us/howto/wp7/basics/use-a-pin-to-lock-my-sim-card.aspx>.

Extra Tip: Make sure that you turn off cookies and the auto-fill option that finishes passwords and other form data as you start to type a word. If your mobile device automatically enters passwords and login information into websites you visit frequently, it is important to disable that feature in case the phone falls into the wrong hands. Auto-fill is convenient, but it can also be a privacy threat. To get back some of the convenience that auto-fill offers, utilize third-party apps (mentioned elsewhere) to manage and protect passwords with a higher level of security. Using them is not as secure as turning off auto-fill altogether, but it's one way to strike a good balance.

3. Enable Remote Tracking and Wiping Capabilities.

A good IT department won't allow mobile phones out of their site prior to taking most of the steps listed in this document (by definition, then, only about 5% of IT departments can be considered good). The minimum requirements, however, are the use of passwords, remote wipe and remote tracking. Even if your company does not take these steps, you should, as it could mean losing your job if company data is breached on your mobile phone (or losing your identity if you use it personally).

Remote wipe means that if your phone is lost or stolen, you can remotely clear all of your data – including e-mail, contacts, photos, videos, texts, and documents – off of the handset, immediately eliminating the risk posed by loss or theft (as long as your password holds up long enough for you to remotely track and retrieve or remotely wipe the mobile phone).

Remote tracking means that as long as the power on your mobile phone remains on, you can physically track the location of the phone (thanks to the GPS inside). This feature has actually been used to catch criminals in action.

If you are utilizing a company mobile phone, it is probably wise to let your IT department set this feature up for you. This can be done in most of the major operating systems (those listed above) as well as in Microsoft Exchange (assuming you have an Exchange account). Those people without Exchange accounts, IT departments or time to wait around for an answer, have simpler and speedier options.

- ☑ **BlackBerry, Android and Windows Phone 7:** If your OS is included here, you have several options, as you can find robust third-party applications that allow you to remotely wipe your device. [Lookout Mobile Security](#) is one such example, and was

recently one of PC World's Top 100 apps. The basic version is free and the Premium version adds functionality like Remote Wipe, Privacy Scans and App Reports (see later risk areas). It also enables you to track a lost device through GPS, back up your data over the air, and even scan for viruses. It's very inexpensive for the security it provides.

- ☑ **Apple iOS:** iPhone's remote wipe is easy if you are a Mobile Me user, and a bit more work if not. Non Mobile Me users: If you have iOS 4.2 or higher, download the Find My Phone app from the App Store, and enable it in *Mobile Me* (in the *Settings* app). If you lose your phone, you can log in using [Mobile Me](#) and track it, display a message on the home screen, or wipe out the data completely. Mobile Me Users (and for use with older versions of the iOS): Once you have a paid Mobile Me account, which costs \$99 a year for a suite of services, you are ready to start. First, enable the Tracking function in *Settings*, then *Mail*, *Contacts*, *Calendars*, and clicking *Fetch New Data* and then *Enable Push*. Next, return to the *Mail*, *Contacts*, *Calendar* screen and select your Mobile Me account. Use the same [Mobile Me](#) link to test the tracking on your phone (which will also let you know that it is set up correctly for remote wipe (if you can see your phone on the map, you are all set to go)).

Remote tracking is also handy when you forget where you left your phone last. Looking on the map, I could tell where in the house I'd left it. That's a slightly unsettling piece of privacy itself, but that's discussed in a different book.

4. Install Security Software



Hackers and advertisers target their malware (viruses, worms, Trojans, botnets) and adware at the operating systems with the greatest adoption in the market (iOS, Droid, BlackBerry and, as always, Windows). In the coming months, more than 1 in 2 Americans will be utilizing a Smartphone, making it a very attractive target for the types of attacks we have been preventing on our computers for the past 10 years. The trick for the fraudsters is getting software on your phone that turns control of your device over to them. They might do this by getting you to click an enticing link (which downloads malware) or installing a seemingly useful App that is meant to siphon your information back to their waiting servers.

Here are some common signs that signal the possible presence of spyware on your Smartphone:

- Your bill shows higher data usage rates than expected.
- Your bill shows text messages to unknown numbers.
- Your battery is warm even when you aren't surfing or talking on the phone.
- Your phone flickers when not in use, or exhibits other non-typical behaviors.
- You notice a significant drop in performance or a much shorter batter life.

These types of attacks have many sources, including MMS texts, email links, infected

software from dodgy websites and even compromised code from legitimate App stores. Most App stores don't take the time to vet every application they offer for security, and some malware is bound to slip through the cracks. Part of the answer is discussed below (Step 6), but for a more proactive course of action, here are a few suggestions for third-party Smartphone security software:

- ☑ **BlackBerry, Android, and Windows Phone:** Consider Lookout (discussed above) to give you some additional security and scanning tools. Lookout will scan your phone for malware/spyware, and even examine downloaded applications (though only for known viruses, not for risky apps). It's somewhat difficult for security software to detect rogue SMS or MMS scripts, so don't open that MMS unless you absolutely know who it's coming from. Other options for Smartphone security software include Symantec, Mobile Defense and others.
- ☑ **Apple iOS.** Apple doesn't really have many third-party anti-virus apps available for the iOS. Instead, Apple relies on their stringent App Store approval process and operating policies to discourage malware. Considering the sheer number of apps out there, and the number of new apps being added every day, some malware is bound to slip through the cracks. There is just no way to eliminate the risk of human error, and at this point, that is the crux of the app approval process. You might try the Trend Smart Surfing app, which blocks access to Websites known to contain malware and potential phishing attacks. As iOS continues its march into the corporate world, Apple and third party security software will be forced to address this platform.

Even if you don't enable remote wipe or remote tracking, you still have options. If your phone goes missing, you should contact your wireless provider (AT&T, Verizon, Sprint, T-Mobile) and have them immediately shut down service. This is a pretty easy way to keep a thief or opportunist from using the phone or running up charges. You may not have remote wiping capabilities, but they just might.

5. Load Data with Discretion.

The best way to protect sensitive data from being stolen off of a Smartphone is to never put it there in the first place. A Smartphone is pretty much the same thing as your computer, except that it doesn't have as strong of a password (in most cases), is much easier to steal (it's smaller), has far less real-world security testing (they've only been available to hack for a couple of years) and has much more untested software loaded on it indiscriminately (in the form of the latest Apps, see Step 6). In other words, your Smartphone is a ticking identity theft and data breach time bomb unless you consciously protect it.

One solution is commonly overlooked: getting in the habit of storing less data on the actual device. The temptation to keep everything with us at all times is attractive, and dangerous. If you don't need to access a confidential spreadsheet, store financials or banking passwords, don't put them on the Smartphone. In fact, this same strategy works for laptops. I can't tell

you how many breached organizations I speak to that had data on a laptop or Smartphone that didn't need to be there.

If you are using Cloud Computing Services like Salesforce.com, DropBox, Evernote and other centralized storage devices, make sure the passwords that allow access into those applications are longer than 8 characters and use letters, numbers, symbols - both upper and lower case and can't be found in a dictionary or your Facebook profile. If you are storing passwords, make sure you utilize an encrypted password program like 1Password (my favorite) that requires at least one additional level of password encryption before giving access to all of your login information.

Extra Tip: When you are finished using your phone and are planning on giving or throwing it away (or returning it to the I.T. Department or even stuffing it in a drawer), make sure you completely wipe all of the data off of the phone. This could include removing the SIMM card and erasing any internal memory on the device. Remote wipe (see above) is an efficient and effective way to perform this function.

6. Minimize Unnecessary Application (App) Spying

How do you know that the application (App) you are downloading and allowing to access your Smartphone (and all of the data on it) is legitimate? In some cases – you don't. And how do you know that someone else hasn't installed a tapping App on your mobile phone without your knowledge? The practice is very common, whether the secretive App installation is done by a disgruntled spouse, a nosy employer, a sophisticated competitor or thief who convinces you to click on a malicious link and install spying software.



a

Recently, I was asked to help with a case of domestic abuse: the husband had installed a Mobile Tapping App (like computer spyware or a key-logger) on his wife's phone prior to their divorce. During the divorce proceedings, he listened to every conversation, read every email and text sent from her phone, and could even control her calendar and applications. Because of GPS tracking, he always knew where she was. When she switched to a new phone number and iPhone, iTunes must have synced the malicious software to the new phone along with all of the legitimate programs – allowing the abusive husband access to the new phone and continue stalking her. To see a scary video demo of mobile phone tapping software visit www.sileo.com/tapping-cell-phones.

Cell phone tapping software (which is nothing more than an invisible App that doesn't show up on your home screen) allows the user to perform all of these tasks without your ever knowing it:

- Silently record the entire content of all SMS text messages, emails and web browsing (allowing them to read all of your incoming and outgoing text messages)

- Log information about each call (so that they know who you called, when and for how long)
- Provide actual GPS positions (so that they know where you are anytime your phone is on)
- Receive a text message when someone uses the cell phone so that the spy can call in and listen to everything being said (every conversation you have can be overheard and recorded)
- Turn the cell phone into a remote listening device, even when the phone is not open or in use (allowing the spy to listen in on conversations anytime your cell phone is near)

But rogue applications aren't just installed on your Smartphone by angry ex-partners. Just as viruses and spyware are installed on computers, so are they installed on phones, except that it is much easier because the average Smartphone user installs numerous Apps without really thinking about it or verifying the legitimacy of the software. You see, when you install an App, you are often giving them permission to utilize your personal information, often including your mobile phone ID, phone number, text messages, called numbers and other personal information. Of course, you never know this because few of us actually read the Terms of Agreement when downloading the App.

Apple tries to minimize the number of malicious applications using a centralized App Store screening process to certify the security of every App, but they do acknowledge that malicious applications have snuck through. The Android Marketplace and Blackberry App World place users in charge of their own security, which means that you have almost no protection. Of course all of the application stores will remove false apps when they are aware of them, but it can sometimes be too little too late.

In addition, some of the very most popular and legitimate Apps are spying on you as well. They don't intend to steal from you, but they are collecting, aggregating and selling your private information for a profit. After examining over 100 popular apps, the Wall Street Journal found that 56 of them transmit the phone's unique device ID to companies without the user's knowledge. Forty seven of the applications transmitted the phone's actual location, while five sent other personal information such as age and gender. This shows how many times your privacy is potentially compromised without your knowledge, just by playing paper-toss. Here are a few of the culprits:

- Textplus 4 is a popular text-messaging app. It sent the unique phone ID to over 7 different ad companies.
- Pandora, a popular music application for both smart-phones and computers sends age, gender, location and phone ID to many advertisers.
- Paper Toss sends your phone ID to 5 different advertisers.



Smartphone providers such as Apple and Google state that they make sure applications get approval from users in order to transmit this type of information, but we aren't actually seeing this happen in the real world. Google, creator of the Android, does not monitor their

apps and what they are transmitting at all. Neither Google nor Apple requires their apps to have privacy policies, and 45 of the 100 apps examined didn't have one. Just a few months ago, two of the most popular gaming Apps on the Android platform were produced by the government of North Korea. Not exactly my first choice of countries with which to share my data.

Smartphone security is still in its early stages, but will quickly become more sophisticated as these little devices drastically increase productivity, connectivity and communication. In the meantime, regardless of which Smartphone you use, keep the following in mind when installing that new App:

- ☑ Never open email, text, IM, Facebook or other attachments from untrusted sources.
- ☑ Never click on shortened links unless you are very confident they are from a trusted source.
- ☑ Apps, even legitimate ones, are capturing and transmitting a variety of your personal information. If you are using smart-phone apps, your information is being transmitted.
- ☑ Get your Apps from a trusted source; don't just install the latest fad. I tend to stick with App stores that are monitored and written up in journals.
- ☑ Paid Apps tend to transmit less personal data than free Apps. After all, the free Apps have to make money somehow!
- ☑ If an App gives you the option to opt out of information sharing, take it.
- ☑ Some malicious Apps are recognized and quarantined by Smartphone security software (see Step 4).
- ☑ As Smartphones begin to allow you to restrict data sharing on an App by App basis (like in the location section below), make sure you go in and customize your settings.
- ☑ When downloading applications, do your research first. Has the App been reviewed by a reputable source (Macworld, PC Magazine, PC World, WSJ, NYT)? This doesn't guarantee anything, but it's a start.
- ☑ Avoid the latest trendy App until it has been out long enough to earn the trust of reputable reviewers.
- ☑ If an App requests permission to access your personal data (text messages, cell number, current location, etc.) make absolutely certain you want to share that information.
- ☑ If you no longer use an App, or are suspicious about it, remove it from your phone.
- ☑ Be advised: even if the application you are downloading and accessing does ask for your permission to gather location information, they probably don't disclose who they are sending it to or how they are using it.

7. Turn on Data Encryption

Encryption, or the practice of scrambling your data behind sophisticated password protection, isn't as widely available for Smartphones as it is for computers. BlackBerry has been providing advanced, device-wide encryption for some time, which is what arguably makes it the most secure Smartphone operating system. The iPhone, Droid and Windows7 arguably give you some level of encryption when you turn on the passcode feature (Step 2). In addition, it is increasingly possible for you to encrypt (via password) your SIMM card. Consult your user manual or the website of your mobile phone provider for further details.



As encryption becomes more sophisticated for these platforms and operating systems, implement security as you would on your computer systems. In the meantime, use password and individual file encryption programs (e.g., 1Password) to protect the most sensitive data on the phone.

Extra Tip: Don't "jail break" your Smartphone, as this not only makes it susceptible to malware and voids the warranty, but it pretty much makes any encryption available on the phone useless. Once you open the back door, so to speak, you are letting everyone in, not just a new phone carrier. Jail breaking refers to the practice of cracking the security on your mobile phone in order to utilize a different carrier, e.g., using T-Mobile on your iPhone or perform other functions not allowed by your service provider (tethering, App purchases, etc.).

8. Hold off on Mobile Banking and Investing

Because of all of the risks of data leakage posed by your Smartphone, I don't yet recommend using online banking and investing Apps or browser-based banking. For now, the security on mobile phones is in its infancy and the attackers are many steps ahead. All it takes is for one rogue App to funnel your brokerage login credentials to an outside source and your net worth could be eliminated. The risk, for now, is too high. Contain your online banking and brokering to a home-based or business-based computer system with all of the proper security cautions (strong passwords, anti-virus and anti-spyware software, firewall protection, updated OS patches, etc.).

9. Customize Your Geo-Tag and GPS Settings

Geo-tagging allows others to track your location even though you don't know it. With the increased use of Internet-enabled mobile devices such as the Blackberry, Droid and iPhone, geo-tagging has seen a huge increase in popularity. For example, when social media users take a picture or video and upload it to their page, they are probably transmitting location data without knowing it. With the ability to quickly add GPS information to media, smartphones make geo-tagging a simple task.

Simply, geo-tagging is where location or geographical information, such as your GPS coordinates, are added and embedded to different types of media (photo and movie files, for example). Invisible to the naked eye and the casual observer, geo-tags are part of the meta-data, or underlying data about the data, that accompanies each file. Examples of meta-data include when the file was created or modified, by whom, using what device and software. This data is often loaded on to your computer along with the original file. Browser plug-ins and certain software programs can reveal the location information to anyone who wants to see it.

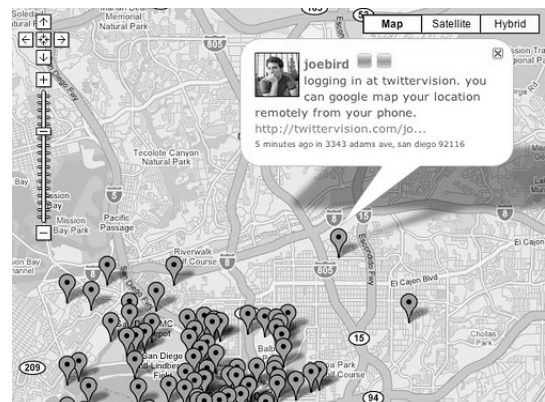
Twittrvision makes great use of geo-tagging. Twittrvision combines Twitter with Google Maps to create a real time display of tweets across a map. It also has a 3D mode that displays a globe of the Earth, which spins to pinpoint arriving messages from Twitter.

So, who would want to know where you are?

While most of the uses are not fully apparent yet, your real-time location can reveal your home address, work address, places you visit often and at what time of day. Geo-tags make it very easy for friends, relatives, bosses, spouses, parents, enemies, law enforcement, stalkers, and thieves to know exactly where you are.

Telling everyone on your Facebook status that you are out for the evening can invite burglars; geo-tagging can do the same without you updating your status in any way. By taking a picture at the Barry Manilow concert and uploading it to your twitter account, you are broadcasting the fact that you are probably over 40, away from home and, thanks to the geo-tag, exactly how far away you are.

The problem with geo-tagging is that since it is not visible to the naked eye, most people don't even realize they are sharing their location data. So what can you do if you don't want to transmit your location data?



Keeping location data private can be difficult, but start here:

- ☑ Understand that anytime you take a picture, video or post an update from a networked device (somehow connected to the internet), your location is probably being appended to the file, even though it is hidden from you. As with all things technological, there are advantages and disadvantages to all features. Location based services also allow you to use handy tools like maps; give you Big Brother-like power in tracking your kids' whereabouts, and allow thieves to burgle you when no one is home using tools like Foursquare and Facebook Places.
- ☑ **Apple iOS:** Disable geo-tagging application by application on your **iPhone 4**. In your phone, go to *Settings, General, Location Services*. Here you can set which applications can access your GPS coordinates, or disable the feature entirely (which could cause you problems using maps, restaurant finders, etc.).
- ☑ **BlackBerry:** Disable geo-tagging for photos on your **BlackBerry**. Go into picture-taking mode (*Home Screen*, click the Camera icon), press the *Menu* button and choose *Options*. Set the *Geo-tagging* setting to "Disabled". Finally, save the updated settings. In some cases, these menus appear under the *Location* icon or alternatively under the *Settings* menu. Consult your user's manual for specifics.
- ☑ **Android:** Disable geo-tagging for photos on your **Droid**. Start the Camera app (this is the menu on the left side of the camera application; it slides out from left to right). Select *Location* and make sure it is set to "Off". In other cases, get into Camera mode and then select *Menu* and *Settings*.
- ☑ **Windows Phone:** Disable geo-tagging for photos on your **Droid**. Go to *Settings, Applications, Pictures & Camera*, and then toggle the "include location (GPS) information in pictures you take", to the *Off* position.
- ☑ Although Facebook does remove geo-tags from uploaded photos (at the time of this writing), other social networking sites do not. Look into your privacy settings and turn off location sharing. As mentioned above, you can generally turn this feature off in your camera or phone as well.
- ☑ Take particular care if you are uploading photos to a website where strangers will see them — such as Craigslist or Ebay.
- ☑ Consider installing a plug-in on your browser to reveal location data — such as Exif Viewer for Firefox or Opanda IExif for Internet Explorer, so you can see geo-tagged data for yourself.
- ☑ Take the time to stay informed about geo-tagging and other types of new technologies. By knowing what is out there, you can ensure the next photo or piece of media you upload won't share your location with the World Wide Web.

10. Use Tethering and Mobile Account Alerts to Your Advantage

Smartphones are not just a risk in the data protection game; they can also be used as a tool to lower your risk. Here are two examples of ways that you can put your Smartphone to work in the fight against data theft.

Smartphone Tethering

Another major source of data theft is Wi-Fi hotspot usage. Most Free hotspots do little to protect the data that you transmit over the wireless network. In fact, many home and company wireless networks are not set up to provide a secure connection to the internet and are, therefore, no safer than those you access for free in cafés, airports and hotels. Just say no to using free Wi-Fi hotspots, on your phone and your laptop. The most common form of exploitation associated with hotspots are “man-in-the-middle” attacks where a spy intercepts the transmission between your wireless network card and the cafés wireless router or modem.



Using a legal, free and simple-to-use tool like Firesheep, a thief (or competitor/law enforcement, etc.) can sit next to you in a café and “sniff” your connections. Luckily, your Smartphone can provide a proactive way to help you protect your connection to the Internet when surfing wirelessly.

Tethering connects your computer to the Internet using a Smartphone (or Internet-enabled cell phone). **It increases security because the mobile transmission between your cell phone and the cell tower is encrypted (scrambled) and hard to intercept.** Therefore, when you use your Smartphone to surf the web, you are accessing a protected connection that probably can’t be sniffed. The connection might be slightly slower than a traditional Wi-Fi hotspot, but it is also much safer. The Smartphone can be tethered in three basic ways:

1. With a *tethering* cable (usually USB to Smartphone connection). This is the safest option because it is a direct connection between your phone and your computer, eliminating any wireless sniffing between those two devices.
2. With a Bluetooth wireless connection. If you don’t use an encrypted Bluetooth connection, spies can sniff the data as it crosses from your computer to your phone. In addition, turning on Bluetooth functionality opens up one more door for hackers to gain access into your system.
3. Wi-Fi. If connected through Wi-Fi, the tethering feature is usually called a mobile hotspot, and can often connect to multiple devices (unlike wired or Bluetooth, which generally handle only one connection). Again, if you utilize Wi-Fi tethering, you need to make sure that the connection between your computer and the mini hotspot is encrypted so that data isn’t intercepted before it heads to the Internet.

Most Smartphones are equipped with software to provide tethered Internet access via Bluetooth or a USB cable. Tethering may be provided as part of your monthly data plan, but I wouldn’t count on it. I tend to use tethering anytime I’m sending emails, dealing with financial institutions or handling sensitive data. If I’m simply surfing news or sports sites, then I’m more comfortable using the free Wi-Fi connections (as long as my computer is

protected with a firewall against hackers gaining access into my laptop via file sharing over wireless). I generally also log in as a different user on the laptop with very restricted access. This will minimize collateral damage if a thief does back their way in to your connection. Finally, I carry a laptop with very little sensitive data on the hard drive to minimize what can be lost or stolen.

For added security, set up a Virtual Private Network (VPN) that protects the data from the moment it leaves your device to its final destination. A VPN provides secure access to an organization's network and allows you to get online behind a secure layer that protects the data being transmitted back and forth. If you have access to a VPN, I highly recommend that you use this when using Wi-Fi.

Extra Tip: When you are not using Bluetooth or Wi-Fi, turn them off. The most likely way that your smartphone can be compromised is by downloading malware concealed in a file or App. Both Wi-Fi and Bluetooth provide a doorway into your mobile phone (especially when they are set up without security in mind). When they are turned on, they actively *try* to connect to other networks, even when those networks are run by dishonest people. In addition, if tethering is set up incorrectly, it can give the criminal access not only to your Smartphone, but also to your computer. When not in use, turn them off and eliminate chances of foul play.

Mobile Account Alerts

Virtually every major credit card company, bank, mortgage broker and investment firm will allow you to set up account alerts that notify you anytime a transaction is made on your account. Spend \$5 on coffee; you get an alert, either by email or text (in either case, on your Smartphone). The alerts allow you to keep frequent tabs on financial transactions, increasing the chances that you will detect fraud quickly. Account alerts are one of the most powerful and least expensive (free) methods for monitoring your valuable financial accounts.

You generally set up account alerts by logging in to your online account (e.g., where you do your online banking, investing, etc.) and going into the alerts or notification section of the website. If you have trouble finding it, contact the financial institution and a representative will help you set up this feature.

Account alerts notify you automatically by e-mail or text message (to your cell phone) when a transaction is made on your account. For example, if you make a purchase on your credit card, an alert will automatically be sent to you detailing how much you spent, where you spent it, and on what date. The alert will also tell you when a payment is due or has not been received on time, or when private information (like your address) has been changed on the account (often, a sign of fraud). Alerts are a simple way to keep track of credit card usage, bank transfers, low account balances, investment moves, and a handful of other helpful tasks, without doing any extra work. You just verify that each e-mail or text is legitimate. If it isn't, you call the financial institutions and inform them that you think you are the victim of fraud. They will help you handle it from there. By catching the signs early, you eliminate your liability and cost.



A Crash Course in Expanding Mobile Security into the Workplace

Smartphones are so similar to laptops that they serve as a good springboard inside of corporations to build better data privacy habits. Develop a language and framework of security for a

Smartphone and it's easily expanded to other platforms, like laptops.

The most important step of all inside of a corporation is to train your people to detect social engineering (manipulation) and fraud. Now that you have taken the steps to technologically protect your Smartphone, you still need to protect the human beings using it. At the heart of every data theft is a poorly trained user. Here are some points to consider:

- ☑ Research, define and log what is at risk on your mobile data devices.
- ☑ Train on acceptable use of mobile data devices within your company.
- ☑ Control exposure and eliminate unnecessary transport of mobile data.
- ☑ Verify that all systems are digitally secure, not just Smartphones.
- ☑ Encrypt individual files, hard drives, SIMM/SD memory cards as required.
- ☑ Protect mobile devices with security software and strong passwords.
- ☑ Defend online communications with secure Wi-Fi, firewall and SSL email.
- ☑ Physically secure your mobile device while traveling (e.g. hotel safes).
- ☑ At airport security, don't leave your Smartphone unattended on the belt.
- ☑ Utilize remote tracking/wiping admin software to centralize management.
- ☑ Destroy sensitive digital files after they have served their purpose.
- ☑ Take the proper recovery steps if a mobile device has been stolen:
 - Report it to local authorities.
 - Report it to your company.
 - Alert anyone who may be affected.
- ☑ Prepare for a legal compliance battle, suing customers and bad press.

A Smartphone can be a highly effective and efficient tool, for personal and corporate users. But like any powerful piece of equipment, you must take the time to protect it. The more you think of your Smartphone as a computer and the less you think of it as a phone, the more secure you will be. Take steps now to protect this asset.



John Sileo's identity was stolen from his business and used to **embezzle almost a half-million dollars** from his clients. While the thief covered his crimes using Sileo's identity, John and his business were held legally and financially responsible for the felonies committed. The **breach destroyed John's corporation** and consumed two years of his life as he fought to stay out of jail. But John chose to fight back and speak out.

Emerging from this crisis, John became America's leading professional speaker on information survival, including **identity theft prevention**, data breach, cyber security, human manipulation and social media exposure. John is the **award-winning author** of *Stolen Lives*, *The Facebook Safety Survival Guide* and *Privacy Means Profit* (Wiley), and has recently appeared on **60 Minutes** and *Fox and Friends*, for which he is a regular contributor.

John's satisfied clients include the **Department of Defense**, Blue Cross Blue Shield, the FDIC, Pfizer, the Federal Trade Commission, Lincoln Financial, the Department of Homeland Security, AARP, Prudential, the Federal Reserve Bank, and scores of corporations, universities, and associations of all sizes.



Top 5 Smartphone Vulnerabilities

7. Mobile Phone Tapping Software
6. Intercepted Bluetooth and Wi-Fi Connections
5. Text, SMS, and Email Virus & Malware Attacks
4. Physical Theft and Illegal Usage of the Mobile Phone
3. Rogue Applications that Siphon Private Data
2. Legitimate Applications that Siphon Private Data
1. Theft of Files, Contacts, Passwords and Credentials